IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX INC. and SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,	§	
	§	
Plaintiffs,	§	
	§	**CASE NO. 6:12-CV-855**
vs.	§	
	§	
APPLE, INC.,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION AND ORDER

This Memorandum Opinion construes the disputed claim terms in U.S. Patent Nos. 6,502,135 ("the '135 Patent"), 7,418,504 ("the '504 Patent"), 7,490,151 ("the '151 Patent"), 7,921,211 ("the '211 Patent"), 8,051,181 ("the '181 Patent"), and 8,504,697 ("the '697 Patent") (collectively, "the patents-in-suit"). Also before the Court is Defendant Apple, Inc.'s ("Apple") Motion for Summary Judgment of Indefiniteness (Docket No. 148). On May 20, 2014, the parties presented arguments on the disputed claim terms at a *Markman* hearing. For the reasons stated herein, the Court adopts the constructions set forth below and **DENIES** the Motion for Summary Judgment.

BACKGROUND

VirnetX, Inc. ("VirnetX") and Science Applications International Corporation ("SAIC") assert six patents against Apple. The '135 Patent discloses a method of transparently creating a virtual private network ("VPN") between a client computer and a target computer. The '504 and '211 Patents disclose a secure domain name service. The '151 Patent discloses a domain name service capable of handling both standard and non-standard domain name service queries. The

'181 Patent discloses a method of establishing a secure communication link. The '697 Patent discloses a method of communicating between network devices.

The patents-in-suit are all related; Application No. 09/504,783 ("the '783 Application") is an ancestor application for every patent-in-suit. The '135 Patent issued on December 31, 2002, from the '783 Application. The '151 Patent issued from a divisional of the '783 Application. The '181 Patent issued from a divisional of a continuation-in-part of the '783 Application. The '504 Patent issued from a continuation of a continuation-in-part of the '783 Application. The '211 Patent issued from a continuation of the application that resulted in the '504 patent. The '697 Patent issued from a continuation of a continuation of the application that resulted in the '211 Patent. The '135 and '151 Patents share a common specification, as do the '504, '211, and '697 Patents.

The Court has already construed some of the terms at issue. *See VirnetX, Inc. v. Microsoft Corp.*, No. 6:07-cv-80, Docket No. 246 (E.D. Tex. July 30, 2009) ("*Microsoft*"); *VirnetX, Inc. v. Cisco Systems, Inc., et al.*, No. 6:10-cv-417, Docket No. 266 (E.D. Tex. Apr. 25, 2012) ("*Cisco*"); *VirnetX, Inc. v. Mitel Networks Corporation, et al.*, No. 6:11-cv-18, Docket No. 307 (E.D. Tex. Aug. 1, 2012) ("*Mitel*"). The *Microsoft* case involved the '135 Patent; the *Cisco* case involved the '135, '504, '151, and '211 Patents; and the *Mitel* case involved the '135, '504, and '211 Patents.

APPLICABLE LAW

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In claim construction, courts examine the patent's intrinsic evidence to define the patented invention's scope. *See id.*; *C.R. Bard, Inc. v. U.S.*

Surgical Corp., 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). This intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard, Inc.*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312–13; *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can also aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314–15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *see also Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* Also, the specification may resolve ambiguous claim

terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex, Inc.*, 299 F.3d at 1325. But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.'" *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *see also Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is "'less significant than the intrinsic record in determining the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard, Inc.*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition is entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

Apple also contends that some claims at issue are invalid for indefiniteness. A claim is invalid under 35 U.S.C. § 112 ¶ 2 if it fails to particularly point out and distinctly claim the subject matter that the applicant regards as the invention. The party seeking to invalidate a claim under 35 U.S.C. § 112 ¶ 2 as indefinite must show by clear and convincing evidence that the claim, viewed in light of the specification and prosecution history, does not "inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2129, 2130 n.10 (2014); *see Intellectual Prop. Dev., Inc. v. UA-Columbia Cablevision of Westchester, Inc.*, 336 F.3d 1308, 1319 (Fed. Cir. 2003).

LEVEL OF ORDINARY SKILL IN THE ART

The parties agree that a person of ordinary skill in the art would have a master's degree in computer science or computer engineering as well as two years of experience in computer networking and computer network security.

AGREED CLAIM TERMS

In the Joint Claim Construction Chart (Docket No. 113-1, Ex. A) the parties agreed to the construction of the following terms:

Claim Term	Agreed Construction
secure target web site	a secure web site on the target computer
automatically initiating the VPN	initiating the VPN without involvement of a user
DNS proxy server	a computer or program that responds to a domain name inquiry in place of a DNS
automatically initiating an encrypted channel	initiating the encrypted channel without involvement of a user
automatically creating a secure channel	creating the secure channel without involvement of a user
automatically creating an encrypted channel	creating the encrypted channel without involvement of a user
secure server	a server that requires authorization for access and that can communicate in an encrypted channel

DISPUTED CLAIM TERMS

virtual private network (VPN)

Claims 1, 4–7, and 9–13 of the '135 Patent contain the term "virtual private network" or "VPN." VirnetX proposes "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure communication paths between the computers." Apple proposes "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous." The Court previously construed this term in *Microsoft*, *Cisco*, and *Mitel*.

The parties dispute whether the Court's construction should require the VPN to be both secure and anonymous. Particularly, the parties dispute the anonymity requirement. Apple asserts that a VPN requires anonymity[1] and proposes the construction this Court adopted in *Cisco* and *Mitel*, which included an anonymity requirement.[2] VirnetX argues that anonymity is not required and proposes the construction this Court adopted in *Microsoft*, which did not include an anonymity requirement.[3] However, the Court's claim construction order in *Microsoft* made clear that this term requires anonymity, even though the Court did not include the anonymity requirement in its construction. *See Microsoft*, Docket No. 246 at 9 ("[T]he Court construes 'virtual private network' as requiring both data security and anonymity."). For clarity,

[1] At the hearing, VirnetX asked Apple to clarify its position regarding anonymity. Apple explained that it contends anonymity is within the ordinary meaning of VPN, not that the inventors redefined VPN to add an anonymity requirement. Docket No. 174 at 30:5–14. Apple further clarified that it does not assert the inventors disavowed the full scope of VPN as known to persons of ordinary skill in the art. *Id.* at 33:3–5. Finally, Apple stated its position is that an IPSec VPN achieves anonymity. *Id.* at 38:8–13.

[2] In *Cisco* and *Mitel*, the Court construed "virtual private network" as "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous." *Cisco*, Docket No. 266 at 5–8; *Mitel*, Docket No. 307 at 4–6.

[3] In *Microsoft*, the Court construed "virtual private network" as "a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers." *Microsoft*, Docket No. 246 at 4–10.

the Court explicitly added the anonymity requirement to its later constructions of this term in *Cisco* and *Mitel*. *See, e.g.*, *Cisco*, Docket No. 266 at 5. The Court hereby incorporates by reference its reasoning in *Microsoft*. For the reasons stated in *Microsoft* and adopted in *Cisco* and *Mitel*, the Court finds that a virtual private network requires anonymity. *See Microsoft*, Docket No. 246 at 8–9. For clarity, this requirement is explicitly included in the Court's construction in this case. *See Cisco*, Docket No. 266 at 5.

If the Court rejects its position, VirnetX requests the Court to clarify the scope of the anonymity required by the Court's construction. First, it asks the Court to clarify that anonymity is broader than that achieved by the IP-hopping embodiments of the '135 Patent, and is achieved by a tunneled, encrypted VPN. At the hearing, Apple agreed that anonymity is not limited to that achieved by the IP-hopping embodiments of the patent. Docket No. 174 at 42:12–15. It also stated that a tunneled, encrypted VPN can—but does not necessarily—achieve anonymity. *Id.* at 41:25–42:4; *see id.* at 38:21–39:7 (providing an example in which a tunneled, encrypted VPN would not be anonymous). Accordingly, the Court clarifies that anonymity is not limited to that achieved by the IP-hopping embodiments of the '135 Patent, and can be achieved by a tunneled, encrypted VPN.

Second, VirnetX requests the Court to clarify that anonymity is achieved by VPNs known to persons of ordinary skill at the time of the invention. According to VirnetX, since Apple claims anonymity is part of the ordinary meaning of VPN, by definition VPNs must achieve anonymity. However, the Court's conclusion that virtual private networks require anonymity is based on intrinsic evidence in the specification. *See Microsoft*, Docket No. 246 at 8–9. Accordingly, whether a certain VPN achieves anonymity as defined in the patent is a question of infringement for the finder of fact.

For the reasons stated in *Microsoft* and *Cisco* and subject to the above clarifications, the Court construes "virtual private network" as "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous."

generating from the client computer a Domain Name Service (DNS) request

Claim 1 of the '135 Patent contains the term "generating from the client computer a Domain Name Service (DNS) request." VirnetX argues that no construction is necessary. Apple proposes "generating and transmitting from the client computer a DNS request." The Court previously construed this term in *Cisco* as "generating and transmitting from the client computer a DNS request." *Cisco*, Docket No. 266 at 27.

This term appears in the first step of the method recited in claim 1 of the '135 Patent. In that first step, a domain name service ("DNS") request is generated from the client computer. The second step determines whether the DNS request seeks access to a secure web site. VirnetX expressed concern that Apple would use its proposed construction of this term to argue that the second step cannot be performed by the client computer, but only by a separate device. At the hearing, Apple stated it will not make that argument. VirnetX then agreed to Apple's proposed construction. The Court adopts the parties' agreed construction and construes "generating from the client computer a Domain Name Service (DNS) request" as "generating and transmitting from the client computer a DNS request."

an indication that the domain name service system supports establishing a secure communication link

Claims 1, 17, 24, 36, 48, and 60 of the '504 Patent contain the term "an indication that the domain name service system supports establishing a secure communication link." VirnetX argues that no construction is necessary, but alternatively proposes "an indication that the

domain name service system has authorized and supports establishing a secure communication link." Apple proposes "an affirmative signal beyond the mere returning of an IP address, public key, digital signature, or certificate that the domain name service system supports establishing a secure communication link." The parties dispute the meaning of an "indication." In *Mitel*, the Court determined that this term did not require construction. *Mitel*, Docket No. 307 at 10.

VirnetX argues that if the Court construes this term, it should clarify that an "indication" means that authorization is being given to establish a secure communication link. Docket No. 136 at 9. VirnetX points to a description in the specification allowing only authorized users to access a VPN. *Id.* at 9–10. It also argues that the specification disparages conventional domain name services ("DNS") for not differentiating between authorized and unauthorized users. *Id.* at 10. However, the specification's preferred embodiments and characterizations of the prior art do not impose an authorization limitation into the claims. Such an authorization requirement is absent from the claims as drafted. Thus, the inclusion of an authorization requirement is improper.

Apple's proposed construction tracks disclaimers that it alleges occurred during reexamination of the '504 Patent, which occurred after the Court issued its claim construction order in *Mitel*. Apple states that during the reexamination, the PTO rejected the relevant claims because the claimed "indicate" and "indicating" limitations were met in the prior art through the return of digital certificates, encryption keys, and addresses in response to a request for a secure DNS. Docket No. 150 at 10. Apple explains that in response to this rejection, the patentees disputed that any of those prior art features met the claimed "indication" limitations, thereby disclaiming those items from the scope of the term "indication." *Id.* VirnetX replies that Apple

misreads reexamination remarks made to distinguish conventional DNS servers, and argues there were no disclaimers. Docket No. 136 at 10–11.

In response to the rejection during reexamination, the patentees argued:

> the [rejection] applies a much broader construction of 'indication' that encompasses features that neither indicate that the domain name service system supports establishing a secure communication link nor are visible to any users, such as merely returning an IP address, a public key, or a certificate demonstrating authenticity of the source of the public key.

Docket No. 150-14, Ex. 13 at 5. The patentees continued, "[t]he '504 patent specification clearly and unequivocally disclaims merely returning an address or a public key by describing these actions as 'conventional' in the prior art . . . ." *Id.*, Ex. 13 at 6. They further stated, "[n]ever does the specification equate the mere return of requested DNS records, such as an IP address or key certificate, with supporting secure communications." *Id.*, Ex. 13 at 6.

In this response, the patentees clearly distinguished the mere return of requested DNS records, such as an IP address or key certificate, the claimed "indication" terms. Thus, the reexamination response constitutes an unequivocal disclaimer of DNS servers that only return requested DNS records, such as an IP address or key certificate. Accordingly, the Court construes "an indication that the domain name service system supports establishing a secure communication link" as "an indication other than merely returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link."

indicate in response to the query whether the domain name service system supports establishing a secure communication link

Claim 1 of the '211 Patent contains the term "indicate in response to the query whether the domain name service system supports establishing a secure communications link." VirnetX argues that no construction is necessary, but alternatively proposes "indicate in response to the

query whether the domain name service system has authorized and supports establishing a secure communication link." Apple proposes "in response to the query for a network address, affirmatively signaling beyond the mere returning of an IP address, public key, digital signature, or certificate that the domain name service system supports establishing a secure communication link." In *Mitel*, the Court determined that this term did not require construction. *Mitel*, Docket No. 307 at 11.

The issue and arguments regarding this term are identical to those raised for the previous term. Namely, VirnetX's response to a rejection during reexamination of the '211 Patent, which contains this term, is identical in relevant respects to the response to a rejection of the '504 Patent quoted above. *See* Docket No. 150-15, Ex. 14 at 5–6. Further, the parties briefed this term together with the previous term. For the same reasons stated regarding the previous term, the Court construes "an indication that the domain name service system supports establishing a secure communication link" as "indicate in response to the query, other than the mere returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link."

intercept / intercepting

Claims 1, 10, 15, 16, 29, and 30 of the '697 Patent contain the term "intercept" or "intercepting." VirnetX argues no construction is necessary. Apple proposes "access/accessing a communication addressed to another." At the hearing, the parties agreed that this term does not require construction, with the understanding that "intercepting" must mean more than simply "receiving." The Court adopts the parties' agreement and clarifies that "intercepting" means more than simply "receiving." Given that clarification, the Court finds that "intercept / intercepting" does not require construction.

[intercept / intercepting] . . . a request to look up an internet protocol (IP) address

Claims 1 and 16 of the '697 Patent contain the term "[intercept / intercepting] . . . a request to look up an internet protocol (IP) address." VirnetX argues no construction is necessary, but alternatively proposes "receiving a request to look up an IP address and performing some evaluation on the request that is not merely resolving the request." Apple argues no construction is necessary beyond the construction of "intercept" and "intercepting."

The issue and arguments regarding this term are identical to those raised for the previous term. Further, the parties briefed this term together with the previous term. For the same reasons stated regarding the previous term, the Court clarifies that "intercepting" means more than simply "receiving." Given that clarification, the Court finds that "[intercept / intercepting] . . . a request to look up an internet protocol (IP) address" does not require construction.

[determine/determining] . . . is available for a secure communications service

Claims 1, 14, and 16 of the '697 Patent contain the term "[determine/determining] . . . is available for a secure communications service." VirnetX argues no construction is necessary. Apple proposes "determine/determining whether a device is available to establish a secure communication link."

VirnetX complains that Apple's proposed construction impermissibly changes the claim language from "available for a secure communications service" to "available to establish a secure communication link." Docket No. 136 at 15. Apple defends its construction, claiming that the secure communication link is used only after the second device is "available for a secure communication service." Docket No. 150 at 19–20. It asserts that, therefore, determining that a device is "available for a secure communications service" requires a determination that the device is "available to establish a secure communications link." *Id.* Apple also cites the

specification in support of its construction, claiming that it equates the "secure communications service" to the establishment and use of a "secure communication link." *Id.* at 20.

The term "secure communications service" is found in the abstract, the summary of the invention, and the claims. In each instance, its availability is the basis for initiating a secure communication link. *See* '697 Patent, abstract (explaining that the invention is configured to "initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service"); *accord id.* at cols. 8:16–20, 8:33–36; *id.*, claims 1, 16. Thus, the patent describes that to be "available for a secure communications service" is to be available "to establish a secure communication link."

The Court construes "[determine/determining] . . . is available for a secure communications service" as "determine/determining whether a device is available to establish a secure communication link."

domain name lookup

Claims 14 and 28 of the '697 Patent contain the term "domain name lookup." VirnetX argues no construction is necessary. Apple proposes "a lookup service that returns an IP address for a requested domain name to the requester." The parties dispute whether "domain name lookup" requires the return of an IP address.

VirnetX contends that the claims only require looking up a domain name—not also returning an IP address. Docket No. 136 at 16; Docket No. 152 at 8. It argues that requiring the return of an IP address would exclude a preferred embodiment that does not return the true IP address, but sets up a VPN instead. Docket No. 136 at 16. Apple disputes that contention, arguing that an IP address is returned even when a VPN is established. Docket No. 150 at 22.

A "domain name lookup" performs the second step in claimed methods of connecting network devices. '697 Patent, claims 1, 14, 16, 28. The specification discloses the return of an IP address after the first step—intercepting a request to look up the second device's IP address—but before the third step—initiating a secure communication link between the two devices. *See id.* at cols. 39:32–38, 40:31–49. Thus, an IP address must be returned during the second step, which is performed by a "domain name lookup." While VirnetX contends an IP address need not be returned, in the example actually cited by VirnetX, a DNS Proxy returns an IP address to the requestor. *Cisco*, Docket No. 266 at 15. Thus, adopting Apple's construction would not exclude a preferred embodiment.

Accordingly, the Court construes "domain name lookup" as "a lookup service that returns an IP address for a requested domain name to the requester."

secure name service

Claims 2, 22, and 28 of the '181 Patent contain the term "secure name service." VirnetX proposes "a lookup service that returns a network address for a requested secure name and facilitates establishing a secure communication link based on a secure name." Apple proposes that the term is indefinite.

Apple argues that the intrinsic record lacks guidance as to how one of ordinary skill would construe "secure name service," which was coined by the patentees. Docket No. 148 at 9. It states that the term was added to the claims to replace the term "name service," which had been rejected as indefinite by the PTO. *Id.* at 14. Apple contends that "secure name service" is indefinite because the patentees' definition of the term during reexamination relied on another term that Apple asserts is indefinite, "secure name." *Id.*

As explained below, Apple has not met its burden to show that the term "secure name" is indefinite. *See infra* pp. 16–17. Thus, Apple's argument that "secure name service" is indefinite because it depends on the definition of "secure name" fails.

Regarding construction, VirnetX argues that a secure domain name service described in the specification is the preferred embodiment of a "secure name service." Docket No. 136 at 16. First, it asserts that, like the embodiment, the claimed "secure name service" returns a network address. *Id.* However, it contends that the embodiment is not limiting. Thus, it contends that, unlike the embodiment, the network address returned is not required to be secure. *Id.* at 17. Second, VirnetX maintains that, like the embodiment, the claimed "secure name service" must facilitate establishing a secure communication link. *Id.*

Contrary to VirnetX's argument, the specification's disclosure of a secure domain name service is not merely a preferred, non-limiting embodiment—it is the only embodiment. It presents the only objective measure to determine the scope of the claims using "secure name service." Consistent with the Court's previous construction of "secure domain name service," the returned network address must be secure. *See Microsoft*, Docket No. 246 at 31–32; *Cisco*, Docket No. 266 at 17–19. Further, VirnetX's proposal requiring the "secure name service" to facilitate establishing a secure communication link adds a functional limitation that does not help define the term. It is thus rejected.

The Court construes "secure name service" as "a lookup service that returns a secure network address for a requested secure name." Apple's Motion for summary judgment that this term is indefinite is **DENIED**.

secure name

Claims 1, 2, 3, 5, 8, 10, 11, 22, 23, and 24–29 of the ’181 Patent contain the term “secure name.” VirnetX proposes “an authenticated name that can be resolved by a secure name service and can be used for establishing a secure communication link.” Apple proposes that the term is indefinite.

Like the previous term, Apple argues that the intrinsic record lacks guidance as to how one of ordinary skill would construe “secure name,” which was coined by the patentees. Docket No. 148 at 9. It states that in response to an indefiniteness rejection regarding “secure name” during prosecution, the patentees only provided non-limiting examples to define the term. *Id.* at 9–10. Apple further notes that dependent claim 3 of the ’181 Patent specifies that the “secure name” in claim 2 be a “secure domain name.” *Id.* at 11. Thus, it argues, “secure name” must encompass something more than a “secure domain name,” which is disclosed in the specification and has been construed by the Court. *Id.*

VirnetX states that in response to the indefiniteness rejection of “secure name,” the patentees not only provided examples, but also explained the term. Docket No. 156 at 5. It argues that the examiner’s subsequent withdrawal of the indefiniteness rejection is evidence that one of ordinary skill would understand the term’s scope. *Id.* at 6. That scope, it asserts, is that a “secure name” is analogous to a “secure domain name,” but not so limited. *Id.*

“Secure name” does not appear in the specification of the ’181 Patent. Therefore, the claims and prosecution history comprise the relevant intrinsic evidence regarding this term. Dependent claim 3 of the ’181 Patent recites, “[t]he method according to claim 2, wherein the secure name of the second device is a secure domain name.” Thus, “secure name” must encompass something more than a “secure domain name.”

In response to the indefiniteness rejection regarding "secure name," the patentees confirmed that "[t]he claimed 'secure name' includes, but is not limited to, a secure domain name." Docket No. 148-8, Ex. 7 at 9. That response also provided two examples of the term: "For example, a 'secure name' can be a secure non-standard domain name, such as a secure non-standard top-level domain name (e.g., .scorn) or a telephone number." *Id.*, Ex. 7 at 9. Further, the patentees' response explained the meaning of the term:

> [A] 'secure name' is a name associated with a network address of a first device. The name can be registered such that a second device can obtain the network address associated with the first device from a secure name registry and send a message to the first device. The first device can then send a secure message to the second device.

Id., Ex. 7 at 9. Apple's briefing does not address this explanatory passage. *E.g.*, Docket No. 148 at 10 (asserting that, "[i]n responding to the indefiniteness rejection, rather than attempt to define the term, VirnetX simply gave two examples of what it considered to be 'secure names'"). Therefore, Apple does not address how the passage fails to define the term or to differentiate a "secure name" from a "secure domain name." Apple has thus not met its burden of showing by clear and convincing evidence that the term is indefinite.

Regarding construction, VirnetX advances the same arguments for this term as it did for the previous term, "secure name service." Docket No. 136 at 18. In addition, it argues that the secure name is "authenticated" because the specification and file history teach that the secure name can be registered. *Id.* at 18–19. Apple disputes that a secure name is "authenticated." Apple argues that the '181 Patent does not require domain names to be registered, or even contain the phrase "authenticated name." Docket No. 150 at 29.

VirnetX's proposed construction is unsupported. Its requirement that a secure name "can be used for establishing a secure communication link" does not define what the term means and

is rejected. Similarly, the specification does not support the proposed construction's "authentication" requirement. A secure name is not required to be authenticated simply because it is able to be registered. The phrase "resolved by" is vague and introduces an ambiguous concept.

Accordingly, the Court interprets this term in light of the patentees' explanation of the term to the PTO. The Court construes "secure name" as "a name corresponding to a secure network address." Apple's motion for summary judgment that this term is indefinite is **DENIED**.

unsecured name

Claims 1, 26, and 27 of the '181 Patent contain the term "unsecured name." VirnetX proposes "a name that can be resolved by a conventional name service." Apple proposes that the term is indefinite.

Apple advances the same indefiniteness arguments for this term as for the previous term. Apple's indefiniteness arguments for this term fail for the same reasons stated regarding the previous term.

Further, Apple disputes the use of the phrase "conventional name service" in VirnetX's proposed construction. Docket No. 150 at 30. It argues that the '181 Patent does not use that phrase or provide guidance as to how one of ordinary skill would differentiate conventional from unconventional in this context. *Id.* Apple also criticizes that under VirnetX's proposed construction, the definition of "unsecured name" overlaps with the definition of "secure name." *Id.* at 28. That is, it challenges VirnetX's assertion that a conventional name service can resolve "secure names," not just "unsecured names."

To support the inclusion of "conventional name service" in the construction, VirnetX cites a portion of the specification that discloses an unsecured name that is registered with

"conventional domain name services." Docket No. 136 at 19 (citing '181 Patent at col. 52:50–58). VirnetX further explains that the specification does not require "secure names" and "unsecured names" to be mutually exclusive. Docket No. 152 at 8. It points to an embodiment claiming a *non-standard* "secure name" that conventional domain services cannot resolve. Docket No. 136 at 19 (citing '181 Patent, claim 23). It argues that since not all secure names are non-standard, the patent does not foreclose the possibility that a conventional name service can resolve "secure names," not just "unsecured names." *Id.*

As noted with regard to the previous term, the phrase "resolved by" in VirnetX's proposed construction is vague and introduces an ambiguous concept. Thus, VirnetX's proposed construction is rejected. Further, the ordinary relationship between "unsecured name" and "secure name" is that the terms are opposites. VirnetX's cited embodiment accords with this ordinary relationship; it does not evidence a departure from it. VirnetX provides no evidence that the patentee redefined "secure names" and "unsecure names" to overlap. Therefore, one of ordinary skill in the art would interpret "unsecured name" and "secured name" to be mutually exclusive.

Accordingly, the Court construes "unsecured name" as "a name corresponding to an unsecured network address." Given that this construction defines the scope of the term, it is not indefinite. Apple's Motion for summary judgment that this term is indefinite is **DENIED**.

securely communicate

Claims 1, 24, 26, and 29 of the '181 Patent contain the term "securely communicate." VirnetX argues that no construction is necessary, but alternatively proposes "communicate with data security." Apple proposes "send a message over a secure communication link."

Apple states that the specification only refers to sending messages over a secure communication link. Docket No. 150 at 23. Therefore, Apple concludes, "securely" necessarily

means a secure communications link is required for sending or communicating a message. *Id.* at 24. VirnetX disputes the inclusion of "secure communications link" in Apple's proposed construction, arguing that the phrase is already a separate claim limitation. Docket No. 136 at 20. It argues that, to the extent construction is necessary, this term should be construed simply to acknowledge that "securely" refers to data security. *Id.*

As VirnetX correctly states, the claims already recite that messages are sent over a secure communications link. *See* '181 Patent, claim 1 (reciting receiving a message from a second device "to securely communicate" with a first device and then "sending a message over a secure communication link"). In its constructions of "secure communication link" in *Cisco* and *Mitel*, the Court held that the term "securely" referred to data security. *Cisco*, Docket No. 266 at 10–13; *Mitel*, Docket No. 307 at 6–7. VirnetX's alternative construction is consistent with that finding.

Accordingly, the Court construes "securely communicate" as "communicate with data security."

sending a message securely

Claims 24–26 and 29 of the '181 Patent contain the term "sending a message securely." VirnetX argues that no construction is necessary, but alternatively proposes "sending a message with data security." Apple proposes "sending a message over a secure communication link." The issue and arguments regarding this term are identical to those raised for the previous term. For the same reasons stated regarding the previous term, the Court construes "sending a message securely" as "sending a message with data security."

non-secure communication link

Claim 7 of the '181 Patent contains the term "non-secure communication link." VirnetX proposes "a communication link that is not a secure communication link." Apple proposes "a communication link that transmits information in the clear."

VirnetX argues that the prefix "non" applies to the entire remainder of the term, "secure communication link." Docket No. 136 at 21. Thus, it contends that this term encompasses anything that does not meet the Court's construction of "secure communication link." *Id.* The Court previously construed "secure communication link" to require both security and direct communication. *Cisco*, Docket No. 266 at 10–13.[4] Thus, according to VirnetX, a "non-secure communication link" includes communication links that provide security but do not directly communicate.

Apple contends that the prefix "non" applies only to the word "secure." Docket No. 150 at 24. Thus, it contends that this term means a communication link that is not secure, regardless of whether or not it directly communicates. *Id.* It argues that VirnetX's conclusion that an encrypted link could still be deemed non-secure is absurd. *Id.* at 24–25.

The prefix "non" applies only to the word "secure." When the patentees wished to apply the prefix "non" to a phrase lasting more than one word, they made their intention explicit. *See* '181 Patent at col. 49:29–31 (describing a communication link that was not secure and not a VPN as a "non-secure, non-VPN communication link"). Here, the patentees could have applied the prefix "non" to the entire remainder of the term by drafting the term to read "not a secure

[4] In *Cisco*, the Court construed "secure communication link" as "a direct communication link that provides data security." *Cisco*, Docket No. 266 at 10–13. After claim construction, the *Cisco* parties agreed that data security was provided through encryption. In *Mitel*, the Court adopted the *Cisco* parties' amendment and construed "secure communication link" as "a direct communication link that provides data security through encryption." *Mitel*, Docket No. 307 at 6–7.

communication link," but chose not to. Accordingly, the Court rejects VirnetX's proposed construction and adopts the substance of Apple's proposed construction.[5]

The Court construes "non-secure communication link" as "a communication link that transmits information without data security by encryption."

requesting and obtaining registration of a secure/unsecured name

Claims 24–27 of the '181 Patent include the term "requesting and obtaining registration of a secure/unsecured name." VirnetX argues no construction is necessary. Apple originally proposed "requesting and obtaining from a domain name registry service ownership of an secure/unsecured name." However, in its briefing, Apple informed the Court that it no longer proposes a construction. Docket No. 150 at 25. In light of the parties' agreement, the Court finds that "requesting and obtaining registration of a secure/unsecured name" does not require construction.

message

Claims 1, 2, 5, 6, 8, 10–13, 22, 24–26, 28, and 29 of the '181 Patent include the term "message." VirnetX proposes "a unit of information that can be transmitted electronically." Apple proposes "a communication comprising one or more network packets."

Apple argues that the specification equates "messages" with "packets." Docket No. 150 at 26 (quoting '181 Patent at col. 3:14–15 (describing "IP packet messages")). It points to an embodiment that is incompatible with messages that are composed of anything except packets for support. *Id.* VirnetX replies that Apple's proposed construction conflates the information being transmitted (the "message") with the preferred method of delivery (the "packet"). Docket No. 152 at 10. It alleges that if the specification equated messages with packets, then Apple's

[5] The parties agree that "in the clear" describes communication links that are not secure, or unencrypted. Docket No. 136 at 21; Docket No. 150 at 24. In order to clarify for the jury, the Court replaces the phrase "in the clear" with a more concrete synonymous phrase.

cited excerpt from the specification—"IP packet messages"—would be redundant. *Id.* (quoting '181 Patent at col. 3:14–15). For its construction, VirnetX relies on the dictionary definition of "message." Docket No. 136 at 23.

Apple's cited preferred embodiment uses packets to form information messages. But Apple does not cite a disclaimer of the plain and ordinary meaning of "message" that limits it to this preferred embodiment. Accordingly, the Court rejects Apple's proposed construction and adopts VirnetX's proposed construction based on the term's plain and ordinary meaning.

The Court construes "message" as "a unit of information that can be transmitted electronically."

DISPUTED TERMS FOR WHICH PARTIES REST ON PRIOR BRIEFING

For the remainder of the disputed terms, VirnetX and Apple rest on the claim construction briefing from the *Cisco* case. Docket No. 113 at 2; Docket No. 113-2, Ex. B; Docket No. 136 at 14; Docket No. 150 at 19; *See Cisco*, Docket Nos. 173, 182, 192, 209, 366, 424. They raise no new arguments. Because the parties provided no reason to modify the Court's prior constructions and for the reasons stated in the *Cisco* and *Mitel* cases, the Court construes the remainder of the disputed terms as follows:

Claim Term	Court's Construction
Domain Name Service (DNS)	a lookup service that returns an IP address for a requested domain name to the requester
domain name	a name corresponding to an IP address
between [A] the client and [B] the secure server between [A] the client computer and [B] the target computer between [A] a/the first computer and [B] a/the second computer	extending from [A] to [B]

Claim Term	Court's Construction
wherein the secure communication service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device	wherein the secure communication service uses the secure communication link to communicate at least one of video data and audio data extending from the first network device and the second network device
secure communication link	a direct communication link that provides data security through encryption
web site	one or more related web pages at a location on the World Wide Web
secure web site	a web site that requires authorization for access and that can communicate in a VPN
secure web computer	the target computer that hosts the secure web site

Cisco, Docket No. 266; *Mitel*, Docket No. 307.

CONCLUSION

For the foregoing reasons, the Court interprets the claim language in this case in the manner set forth above. For ease of reference, the Court's claim interpretations are set forth in a table in Appendix A and the parties' agreed constructions are set forth in a table in Appendix B. Further, the Court **DENIES** Apple's Motion for Summary Judgment of Indefiniteness (Docket No. 148).

So ORDERED and SIGNED this 8th day of August, 2014.

LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPENDIX A

Claim Term	Court's Construction
virtual private network (VPN)	a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous
generating from the client computer . . .	generating and transmitting from the client computer a DNS request
an indication that the domain name service system supports establishing a secure communication link	an indication other than merely returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link
indicate in response to the query whether the domain name service system supports establishing a secure communications link	indicate in response to the query, other than the mere returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link
intercept / intercepting	No construction necessary. The Court clarifies that "intercepting" means more than simply "receiving."
[intercept / intercepting] . . . a request to look up an internet protocol (IP) address	No construction necessary. The Court clarifies that "intercepting" means more than simply "receiving."
[determine/determining] . . . is available for a secure communications service	determine/determining whether a device is available to establish a secure communication link
domain name lookup	a lookup service that returns an IP address for a requested domain name to the requester
secure name service	a lookup service that returns a secure network address for a requested secure name
secure name	a name corresponding to a secure network address
unsecured name	a name corresponding to an unsecured network address
securely communicate	communicate with data security
sending a message securely	sending a message securely" as "sending a message with data security
non-secure communication link	a communication link that transmits information without data security by encryption
requesting and obtaining registration of a secure/unsecured name	No construction necessary
message	a unit of information that can be transmitted electronically
Domain Name Service (DNS)	a lookup service that returns an IP address for a requested domain name to the requester
domain name	a name corresponding to an IP address

Claim Term	Court's Construction
between [A] the client and [B] the secure server between [A] the client computer and [B] the target computer between [A] a/the first computer and [B] a/the second computer	extending from [A] to [B]
wherein the secure communication service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device	wherein the secure communication service uses the secure communication link to communicate at least one of video data and audio data extending from the first network device and the second network device
secure communication link	a direct communication link that provides data security through encryption
web site	one or more related web pages at a location on the World Wide Web
secure web site	a web site that requires authorization for access and that can communicate in a VPN
secure web computer	the target computer that hosts the secure web site

APPENDIX B

Claim Term	Agreed Construction
secure target web site	a secure web site on the target computer
automatically initiating the VPN	initiating the VPN without involvement of a user
DNS proxy server	a computer or program that responds to a domain name inquiry in place of a DNS
automatically initiating an encrypted channel	initiating the encrypted channel without involvement of a user
automatically creating a secure channel	creating the secure channel without involvement of a user
automatically creating an encrypted channel	creating the encrypted channel without involvement of a user
secure server	a server that requires authorization for access and that can communicate in an encrypted channel